APPENDIX C

INFORMATION SYSTEMS SECURITY OFFICER (ISSO)

TABLE OF CONTENTS

Page

Blank Page

APPENDIX C

INFORMATION SYSTEMS SECURITY OFFICER (ISSO)

C.1 General. This appendix outlines the ISSO's responsibilities and procedures. It also covers defense information service network (DISN) and Standard Army Retail Supply System-Gateway (SARSS-GW) access.

NOTE: Objective Supply Capability (OSC) has undergone a name change and is now called the SARSS-GW. All references to OSC and gateway have been changed and refer to SARSS-GW.

C.2 Security. No classified, personal, or proprietary data is stored or processed at the SARSS-GW; therefore, ISSO personnel, commanders, and managers at all levels are responsible for security in their own data processing operations.

C.2.1 System Access Controls. Log-in identification (ID) and password controls are required by the defense information service network (DISN) and the SARSS-GW. The ISSO, together with the system manager, controls and issues log-in IDs, passwords, and Access Codes. System access must be granted to each standard Army management information system (STAMIS) user, supply and resource manager, and system manager.

C.2.2 User Control of SARSS-GW and Terminal Server Log-In IDs and Passwords. The SARSS-GW and terminal server log-in IDs and are sensitive items and are the responsibility of the individual to whom they are issued. Loss of or compromise of a SARSS-GW or terminal server log-in ID and password must be reported to the local ISSO. The terminal server or SARSS-GW log-in ID and password will only be used by the individual to whom they are issued.

C.3 Access to the SARSS-GW. The SARSS-GW resides at a central location and is linked by modem to SARSS-GW users and supporting supply activities. Access to the SARSS-GW is through the terminal server.

a. Normally, SARSS-GW users access the DISN through a local terminal server maintained by the installation's Directorate of Information Management (DOIM).

(1) The installation ISSO coordinates with DOIM personnel to obtain telephone numbers for the terminal server, where applicable. Terminal servers in the continental United States (CONUS) and outside the CONUS (OCONUS) are

normally password-protected. Local procedures are followed to obtain access through the terminal server.

(2) The installation ISSO coordinates with DOIM personnel to obtain access to the DISN through a terminal server for each SARSS-GW user.

b. STAMIS users and managers at all levels must have a valid log-in identification (ID) and password for access to the SARSS-GW. They must also have a valid log-in and password for the DISN when access is through a terminal server.

c. The installation assigns SARSS-GW log-in IDs and passwords to control access to the SARSS-GW and prevent unauthorized access to system files and processing. Information Systems Security regulations require that passwords be generated by an approved random password generator program.

d. Users may obtain a valid log-in ID, password, and DISN access from the ISSO by submitting a request on a SARSS-GW Security Request Form with the appropriate signatures for approval. See the sample form in figure C.3-1.

SARSS-GATEWAY
SECURITY REQUEST FORM

FOR: SARSS-GW ISSO, Fort Somewhere, VA

This form will be used for requesting access to the SARSS-Gateway. Questions concerning the completion of this form may be directed to the SARSS-GW ISSO, Bldg 1234, ext. 555-5586/1356.

_____ New Request **_____ Delete Request**

NAME: _____ RANK/GRADE: _____
(LAST) (FIRST) (MI)

DUTY TELEPHONE: DSN_____ COM_____
FAX_____

UNIT/ACTIVITY: _____ BLDG# _____ RM# _____
(SYSTEM LOCATION)

WHAT SYSTEM WILL YOU BE WORKING WITH? (SEE BELOW)

CHECK ONE: ULLS ____ SAMS-1 ____ MGR ____

DODAAC: _____ OFFICE SYMBOL: _____

_____
APPROVED BY SUPERVISOR/CDR (PRINT LAST, FIRST, MI, RANK) PHONE

_____
SIGNATURE OF SUPERVISOR/CDR DATE

_____
SIGNATURE OF TERMINAL AREA SECURITY OFFICER (TASO) DATE

_____
SIGNATURE OF SARSS GW ISSO DATE

Figure C.3-1. Security Request Form

e. The ISSO normally handles all requests for log-in IDs, passwords, and DISN access cards.

C.4 ISSO Responsibilities. The ISSO is appointed by the installation and will provide direction and guidance to all assigned or attached personnel. In general, the ISSO is responsible for long-range planning, program oversight, and daily operations of ISSO functions. To be more specific, the ISSO is responsible for:

a. Managing all log-in IDs and passwords for the SARSS-GW application.

b. Maintaining a user database to control SARSS-GW access data.

c. Requesting, issuing, controlling, deleting, managing, and submitting all log-in IDs and passwords to the DECC ISSO for loading to the SARSS-GW application.

C.5 ISSO Tasks. The ISSO has many tasks to perform when managing log-in IDs and passwords for the SARSS-GW application; when maintaining a user database to control SARSS-GW access data; and when requesting, issuing, controlling, deleting, managing, and submitting log-in IDs and passwords to the DECC for loading to the SARSS-GW. These tasks are summarized for you below.

a. When first appointed as the SARSS-GW ISSO, the ISSO must forward the appointment orders and the signature card to the Director of the Defense Enterprise Computer Center (DECC) in Saint Louis, MO.

b. When receiving requests for a valid SARSS-GW log-in ID and password the ISSO must:

(1) Coordinate with the installation's Directorate of Information Management (DOIM) to obtain logins, passwords and telephone numbers for terminal servers.

(2) Generate a DISN Request for forwarding new user information to the DOIM.

c. When managing log-in IDs and passwords for the SARSS-GW application and maintaining a user database to control SARSS-GW access, the ISSO must:

(1) Add users to the ISSO security database.

(2) Review new users and make changes before running reports.

(3) Prepare reports for forwarding new user information to the DECC ISSO.

(4) Print and issue the Password Receipt Form that the user and the DECC ISSO must sign.

(5) Change user names in the SARSS-GW ISSO security database as required

(6) Print the Name Change Request and send it to the DECC SARSS-GW ISSO.

(7) Update user information in the SARSS-GW ISSO security database.

(8) Delete users from the ISSO security database.

(9) Print the SARSS-GW Delete Report and send it to the DECC SARSS-GW ISSO.

d. When performing daily operations, the ISSO must follow e-mail procedures to send new user information.

C.6 ISSO Procedures. The following subparagraphs present the tasks and procedures the ISSO must follow when first being appointed as the SARSS-GW ISSO; when receiving requests for a valid SARSS-GW log-in ID and password and terminal server access; when managing log-in IDs and passwords for the SARSS-GW application and maintaining a user database to control SARSS-GW access; and when performing daily operations.

C.6.1 Forwarding Appointment Orders and Signature Card. When you are first appointed the SARSS-GW ISSO by the installation, you will be given appointment orders like the ones shown in figure C.6-1.

SAMPLE ISSO APPOINTMENT ORDERS

ATZF-LO **22 Aug 2000**

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Duty Appointment

1. Effective 22 Aug 2000, I. M. Whoever, 123-33-3333, is assigned the additional duty as the SARSS-Gateway, Primary Information Systems Security Officer (SARSS-GW ISSO) in the Supply and Services Division, G4/Directorate of Logistics, Ft. Somewhere, VA 23604.

2. Authority: AR 380-19, 1 Aug 90, Information Systems Security.

3. Purpose: To perform duties as SARSS-GW ISSO functions as outlined in AR 380-19, paragraph 1-6d(3).

4. Period: Indefinite.

5. Special Instructions: Individual will familiarize himself with duties outlined in AR 380-19, paragraph 1-6d(3). He is authorized to enforce security policies and safeguards for systems within their purview, to include stopping systems operation if warranted by the seriousness of a security violation.

6. This memorandum of appointment rescinds all previous appointments for this position.

FOR THE COMMANDER:

I. M. Commander
Director of Logistics

DISTRIBUTION:
DECC ISSO, ATTN: WEL52
G4/DOL Phys Security Officer
Individual Concerned

Figure C.6-1. ISSO Appointment Orders

a. You must forward your appointment orders and DD Form 577 (Signature Card) to the Director of the Defense Enterprise Computer Center (DECC) in Saint Louis, MO. You can either do this by mail or fax.

(1) If you want to mail the documents, use this address:

COMMANDER
DECC ST LOUIS
ATTN: WEL52
POB 20012
ST LOUIS, MO 63120-0012

(2) If you want to fax them, use DSN 693-5614 or (314) 263-5614.

b. You may contact the DECC ISSO by calling DSN 693-7934/2903 or (314) 263-2903.

c. Check all passwords that have been generated. If a password is all letters, do not use it.

C.6.2 Generating Passwords for the Installation. The ISSO may use any authorized method of password generation that produces passwords that are a combination of eight (8) alpha, numeric and special characters.

C.6.3 Printing a Master Report of Registered SARSS-GW Users on the Installation. Once you have generated the passwords, you can a master list of passwords for all registered SARSS-GW users on the installation should be created, printed and filed in a secure place. A Master Password List looks like the one shown in figure C.6-2.

05/15/93 Page 1

FT SOMEWHERE MASTER PASSWORD LIST

Last Name	First Name	Rank	Unit	MSC	Phone	Dodaac	Login ID	Password	System
ALLEN	HELLEN	GS9	DOL	TRN-0009	IMMMFS	OFSM0002	pass15		M
ERICKSON	DAVID	SGT	HHC	TRN-0002	WTRNG1	OFSD0001	pass03		D

NOTE: INSTALLATION SARSS-GW SYSTEM MANAGER MAINTAINS THIS LIST. THIS REPORT SHOULD BE CONSIDERED SENSITIVE IN NATURE.

Figure C.6-2. Master Password List

C.6.4 Coordinating with the DOIM to Obtain Telephone Numbers and Request DISN Access. When you receive requests for valid SARSS-GW log-in IDs and passwords and DISN access cards, you must coordinate with the installation's DOIM to obtain telephone numbers for the terminal server, where applicable.

C.6.5 Adding New Users to the ISSO Security Database. To add new users to the database, you should include the following:

LAST NAME	(self-explanatory)
FIRST NAME	
RANK	
MSC	
UNIT	
DODAAC	
PHONE	
LOGIN ID	(see Note 1)
PASSWORD	(see Note 2)
CONTROL	(see Note 3)
SYSTEM	(see Note 4)

NOTE 1: Use this log-in ID structure: "OFSM0001"

O = OSC (SARSS-GW)
FS = Installation Unique Code
M = Type User ID
0001 = Sequence number of each user category

The type user ID in the sample above designates the user as a manager. Here is a list of other user IDs you can use:

2 = SARSS
M = Manager
S = SAMS-1
U = ULLS

NOTE 2: Passwords are generated randomly in accordance with locally established procedures. Passwords should be at least eight characters, one of which must be a number.

NOTE 3: The control number is structured as follows: FS222110001

FS = Installation Unique Code
2221 = Current Julian date
10001 = Last five digits of the log-in ID

NOTE 4: System position is the same entry you use for the user ID.

C.6.6 Reviewing New-User Information and Making Any Necessary Changes Before Running Reports. Once you add users to the database, it is important to review the new-user information in case you need to make any changes before running the reports to sending them to the DECC ISSO.

C.6.7 Preparing Reports and/or Forms for Forwarding New-User Information to the DECC SARSS-GW ISSO Office and to the New User. When you finish reviewing the new-user information and are satisfied that everything is correct, you must prepare reports and/or forms for forwarding new user information to the DECC SARSS-GW ISSO Office and to the new user.

a. You will prepare two separate reports for the DECC SARSS-GW ISSO Office: one called Log-In ID Request that contains log-in IDs for all new users at

the installation and one called Control Passwords for Log-In IDs that contains passwords and control numbers for all new users at the installation.

(1) The Log-In ID Request report containing log-in IDs should looks similar to the one shown in figure C.6-3.

05/22/95 **Page 1**

OSC FT SOMEWHERE
LOGIN-ID REQUEST

LOGIN-ID	LAST-NAME	FIRST-NAME	DODAAC	SYSTEM	CONTROL	PHONE
OFSD0004	WALKER	JOHN	WTRNG1	D	FS3127D0004	TRN-0002
OFSM0002	ALLEN	HELLEN	IMMMFP	M	FS3127M0002	TRN-0009
OFSM0003	SMITH	HAROLD	RMDFP	M	FS3127M0003	TRN-0010
OFSS0002	WILLIS	JOE	WTRNG3	S	FS3127S0002	TRN-0008
OFSU0004	YOUNG	TINA	WTRNG2	U	FS3127U0004	TRN-0007

NOTE: THIS REPORT WILL BE FORWARDED TO DECC OSC ISSO BY MEANS OF E-MAIL OR SECURE FAX. (ISSO@DECC-EMH1.STL.DISA.MIL)

SYSTEM LEGEND:
U=ULLS S=SAMS
1=SAILS 2=SARSS-2A/C
D=DS4 M=MANAGER

Figure C.6-3. Log-In ID Request

(2) The Control Passwords for Log-In IDs report containing passwords and control numbers looks like the one in figure C.6-4.

```
05/22/95                                                Page    1

  DIRECTOR
  DECC-ST LOUIS
  ATTN: WEL03
  ST LOUIS MO 63120-1798

  SUBJECT: LOGIN ID'S FOR FORT SOMEWHERE

                       CONTROL   PASSWORD

                     FS3127D0004 PASS11
                     FS3127M0002 PASS15
                     FS3127M0003 PASS16
                     FS3127S0002 PASS13
                     FS3127U0004 PASS12

  NOTE:   FAX THIS REPORT TO THE DECC SARSS-GW ISSO. DSN 693-5614 OR
COMMERCIAL 314-263-5614.
```

Figure C.6-4. Control Passwords for Log-In IDs

b. You will also prepare a form for the new user called Password Receipt that serves as an acknowledgment of receipt and contains the newly assigned log-in ID and password and information concerning password security for that new user. The Password Receipt form looks like the one shown in figure C.6-5.

OBJECTIVE SUPPLY CAPABILITY
PASSWORD RECEIPT

I hereby acknowledge receipt of the SARSS-GW password associated with the log-in ID shown below. I understand that I am responsible for the protection of this password.

I will not divulge my password to any person, regardless of their security clearance or position, unless authorized by the SARSS-GW Information System Security Officer (ISSO).

I will not allow any other person to operate using my log-in ID, or leave any terminal at which I am "logged in".

I will not exchange my password with any other user for any purpose. I will not use my password to gain access to any data which I am not specifically authorized to use.

I will immediately notify the SARSS-GW ISSO if I believe my password has been compromised in any way.

I will notify the SARSS-GW ISSO if I have any problems with my password.

I understand that any violation of these instructions constitutes misuse of passwords, and I may be subject to having my access removed from SARSS-GW.

I understand it is my responsibility to contact the SARSS-GW ISSO if I am not able to access SARSS-GW.

USER NAME: WALKER JOHN RANK: SGT LOG-IN ID: ofsd0004
UNIT: HHC #1 MSC: TRN DODAAC: WTRNG1 PHONE: TRN-0002

USER SIGNATURE: _____ DATE: _____

ISSO SIGNATURE: _____ DATE: _____

- -

CUT ALONG THIS LINE

LOG-IN ID: ofsd0004 PASSWORD: pass11

NOTE: THE INSTALLATION MAY USE THIS DOCUMENT TO CONTROL PASSWORDS.

Figure C.6-5. Password Receipt

c. When you are ready to prepare the two reports for forwarding the new user log-in ID and password information to the DECC SARSS-GW ISSO Office, you should keep in mind that they are two separate reports that must be accessed, run, and sent to the DECC SARSS-GW ISSO Office separately and in different ways.

(1) You must forward the log-in IDs to the DECC SARSS-GW ISSO Office by e-mail and send the passwords and control numbers to the office by U.S. mail or fax.

(2) If you have e-mail capability, send the above text file to this address: ISSO@STL.DISA.MIL, and furnish a copy to: PPECHENI@STL.DISA.MIL (see e-mail instructions).

(3) If you plan to fax the printed report, use one of these fax numbers: DSN 693-2030 or (314) 263-2030.

C.6.7.1 Preparing the Form for Issuing the Newly Assigned Log-In ID and Password to the User. To prepare the Password Receipt form for you to print, sign, and issue to the user to sign and acknowledge receipt of the newly assigned password and log-in ID, do the following:

a. The Name Change Request report looks like the one shown in figure C.6-6.

05/22/95 Page

OSC FORT SOMEWHERE
NAME CHANGE REQUEST

Login_id	Last_name	First_name	Old_name
OFS10003	WILSON	JENNIFER	BROWN,JENNIFER

NOTE: FAX THIS REPORT TO THE DECC SARSS-GW ISSO.

Figure C.6-6. Name Change Request

b. You must send this report to the DECC SARSS-GW ISSO once it is printed.

C.6.8 Deleting Records from the ISSO Security Database, Printing the SARSS-GW Delete Report, and Sending it to the DECC SARSS-GW ISSO. There may be times when you need to delete records from the SARSS-GW ISSO security database.

a. Print the Request for Delete report so you can verify the information you want to delete before deleting the records from the database and sending the report to the DECC SARSS-GW ISSO.

(1) The Delete selection prints the Request for Delete report that you must send to the DECC SARSS-GW ISSO. This report looks like the one shown in figure C.6-7.

OSC FORT SOMEWHERE
REQUEST FOR DELETE

05/22/93 **Page 1**

DIRECTOR
DECC-ST LOUIS
ATTN: WEL03
ST LOUIS, MO 63120-1978

SUBJECT: OSC USER DELETIONS FOR FT SOMEWHERE

Last_name	First_name	Login_id
WILLIS	JOE	OFSD0002

NOTE: FAX THIS REPORT TO THE DECC SARSS-GW ISSO.

Figure C.6-7. Request for Delete

(2) You must send this report to the DECC SARSS-GW ISSO.

b. Verify the information on the Request for Delete report before going to the next step.